Specifying BYOD Policies with Authorization Logic

Joseph Hallett[1] and David Aspinall[1]

University of Edinburgh

Abstract

BYOD policies are imprecisely specified using natural language. This creates ambiguity, may hide specification problems and make comparison harder. We show how AppPAL (an authorization logic) can be used to formalise BYOD policies. This suggests that the policies could be enforced automatically with greater precision than by relying on users.

1 Introduction

Employees bring their personal devices to work. This is a challenge for corporate IT departments: they want to secure their networks but have limited control over a personal device's software and configuration. To ensure compliance IT departments publish mobile device policies. Employees must agree to follow them if they want to use their personal devices at work. Many policies are specified using natural language which may be ambiguous and hard to check for compliance.

Logics of authorization are languages to express what actions are permissible. Amongst other applicaitons they have been used in access control [6], and to identify problems in electronic health records [7]. *AppPAL* [3] is an instantiation of Becker et al.'s SecPAL [1] language that expresses mobile app installation policies. It makes use of delegation relationships and uses external constraints to formalise policies.

We present excerpts from an AppPAL translation of three BYOD policies: one a security policy from the SANS institute to aid companies in developing their own rules [2], one from an NHS hospital trust [4], and a BYOD policy used at The University of Edinburgh [5]. We show how AppPAL can specifiy BYOD policies making them precise, identifying problems and aiding comparison.

2 Translating Corporate BYOD Policies

Many BYOD policies describe what apps are usable at work. The Edinburgh policy recommends that apps come from a reputable source (though what it means to be *reputable* is left undefined). The SANS policy uses white and black lists of apps written by the IT department, however, the rule is repeated later in their document by another equivalent rule.

Edinburgh: *"Only download applications (apps) or other software from reputable sources."*

```
'edinburgh−policy' says Store can-say App isInstallable if Store sells(App), Store isReputable.
```

SANS: *"The IT Department maintains a list of allowed and unauthorzed applications and makes them available to users on the intranet."*

```
'sans−policy' says 'it−department' can-say App isInstallable.
```

SANS: *"Only approved third party applications can be installed on handhelds. The approved list can be obtained by contacting the IT department, or should be available on the intranet."*

```
'sans−policy' says 'it−department' can-say App isInstallable.
```

The NHS policy makes a distinction between *clinical* and *non-clinical* apps; with each requiring approval through a different group before final approval is given by a commitee. In practice these rules are irrelevant, however, as no group has ever approved an app.

NHS: *"Apps for work usage must not be downloaded onto corporately issued mobile devices (even if approved on the NHS apps store) unless they have been approved through the following Trust channels: Clinical apps; at the time of writing there are no apps clinically approved by the Trust for use with patients / clients. However, if a member of staff believes that there are clinical apps* [···] *ratification should be sought via the Care and Clinical Policies Group.* [···] *Business apps; at the time of writing there are no business (i.e., non-clinical) apps approved by the Trust for use other than those preloaded onto the device at the point of issue. However, if a member of staff believes that there are apps* [···] *ratification of the app must be sought via the Management of Information Group (MIG).* [···] *Following approval through Care and Clinical Policies and / or MIG, final approval will be required through Integrated Governance Committee."*

```
'nhs−policy' says App isInstallable if App isUsable, App isFinallyApproved.
'nhs−policy' says 'cacpg' can-say App isUsable if App isUsableClinically.
'nhs−policy' says 'mig' can-say App isUsable if App isUsableNonClinically.
'nhs−policy' says 'igc' can-say App isFinallyApproved.
```

In all three policies delegation was used to decide whether an employee could install an app. By translating the policies into AppPAL problems become apparent: the Edinburgh policy is *incomplete* as there was no way to determine what stores were reputable, the SANS policy *contains duplicated rules*, and the NHS policy is *redundant* as no app was ever been approved for use. In each case the AppPAL rule was no longer than the natural language policy, and in the case of the NHS policy considerably shorter and clearer.

Some rules appear in different policies with minor changes. Both the NHS and SANS policies regulate the use of mobile devices in cars: by banning the use whilst driving. The SANS policy permits the use of hands-free devices, whereas the NHS policy recommends against them.

SANS: *"Conducting telephone calls or utilizing handhelds while driving can be a safety hazard. Drivers should use handhelds in hand only while parked or out of the vehicle. If employees must use a handheld device while driving,* Company *requires the use of hands-free headset devices."*

```
'sans−policy' says Device mustNotOperate if Device isOwnedBy(Owner)
  where inCar(Device) = true, isDriving(Owner) = true, isUsingHandsFree(Device) = false.
```

NHS: *"For safety reasons, Trust staff must not use a hand held mobile device whilst driving any vehicle.* [···] *the Trust does not recommend using mobile devices in hands-free mode* [···] *whilst driving. "*

```
'nhs−policy' says Device mustNotOperate if Device isOwnedBy(Owner)
  where inCar(Device) = true, isDriving(Owner) = true.
```

When specified in AppPAL the similarities are immediately apparent: the SANS version has an additional constraint but they are otherwise identical.

Other similarities appear when looking at how devices connect to networks. The Edinburgh policy recommends disabling automatic access to open unsecured Wi-Fi networks (though again it does not specify what *secure* actually means). In contrast the SANS policy says what security features are required and that, whilst secured access points are preferred, an open access point may be used with a VPN as a last resort.

Edinburgh: *"Control your devices connections by disabling automatic connection to open, unsecured Wi-Fi networks."*

```
'edinburgh−policy' says Device canConnectTo(AP) if AP isSecure.
```

SANS: *"If mobile workers do require connectivity through public, open, or untrusted WLAN, then users MUST use WLANs using, if available and in this order: WPA(2) encryption, WEP 256 bits (or 128 bits), or finally*

open networks if nothing else is available. Users connected to data networks in an open environment MUST use a VPN connection."

```
'sans−policy' says Device canConnectTo(AP) if AP isSecure.
'sans−policy' says AP isSecure if AP canUseWPA2.
'sans−policy' says AP isSecure if AP canUseWEP256.
'sans−policy' says AP isSecure if AP canUseWEP128.
'sans−policy' says Device canConnectTo(AP) if Device hasVPN(VPN) where connect(VPN) = true.
```

By analysing the similarities in policies a framework of BYOD predicates could be defined that would allow policies to be compared *precisely* using standard terms.

AppPAL can describe complex scenarios in policies. The NHS policy describes when a clinician can use their phone's camera as part of patient care. The rules require obtaining consent (delegation to the patient) as well as clinical approval (delegation to the clinician). As well as helping clarify the policy, the AppPAL rules can aid with compliance: a proof the AppPAL policy was satisfied might act as evidence that proper procedure was followed.

NHS: *"Some mobile devices have the ability to take photographs / videos. This function should not be used for photographs / videos of an individuals care and treatment unless the device has encryption enabled and it is clinically appropriate to do so. If the photography / video facility is used as part of the recording of an individuals care and treatment, the device user must ensure that the consent of the individual has been collected prior to taking any photograph / video.* [· · ·] *A record of the consent must be entered into the individuals care record. "*

```
'nhs−policy' says Device canPhotograph(Patient) if Device isEncrypted, Patient canBePhotographed.
'nhs−policy' says ' clinician ' can-say Patient canBePhotographed
  if Patient hasClinicalNeedForPhotograph, Patient hasConsentedToPhotograph
  where recordedICRConsentForPhotograph(Patient) = true.
'nhs−policy' says ' clinician ' can-say Patient hasClinicalNeedForPhotograph.
'nhs−policy' says Patient can-say Patient hasConsentedToPhotograph if Patient canConsent.
```

3 Conclusions and Future Work

We have shown that natural language BYOD policies contain ambiguities and mistakes. We have also shown how an authorization language, such as AppPAL, might help improve the policies by removing ambiguity, aiding comparison, making delegation relationships explicit and demonstrating compliance. Future work will look in detail at the implementation of a BYOD policy using AppPAL, any problems identified, and the degree to which the policy can be enforced automatically. Automatically inferring when AppPAL policies are incomplete, inconsistent, or have issues with redundancy would help policy designers avoid problems.

References

[1] M.Y. Becker, C Fournet, and A D Gordon. SecPAL: Design and semantics of a decentralized authorization language. *Computer Security Foundations*, 2006.

[2] N.R.C. Guérin. Security Policy for the use of handheld devices in corporate environments, *SANS*.

[3] J. Hallett and D. Aspinall. AppPAL for Android. *Engineeering Secure Software and Systems*, 2016.

[4] G. Kennington, et al. Mobile Devices Policy, *Torbay and Southern Devon Health Care NHS Trust*.

[5] D. Williamson, A. Grzybowski, and S. Graham. BYOD Policy: Use of Personally Owned Devices for University Work, *University of Edinburgh*.

[6] M. Abadi. Logic in access control, *Logic in Computer Science*, 2003.

[7] M.Y. Becker, and P. Sewell, Cassandra: flexible trust management, applied to electronic health records, *Computer Security Foundations*, 2004.